WHAT IS CLAIMED IS:

1. A public-key certificate using system for using a public key certificate which functions, in association with digital signature data of a certificate authority added thereto, as a certificate of a public key for encryption processing, said system comprising:

a person identification certificate authority which executes a person authentication by comparing sampling information which serves as person identification data of a person requesting a public key certificate against a template which serves as person identification data of the person requesting a public key certificate, the template being obtained from a person identification certificate possessed by said person identification certificate authority; and

a certificate authority which issues a public key certificate for the requesting person on condition that the person authentication is established.

2. A public key certificate using system according to Claim 1, wherein said person identification certificate authority obtains sampling information which serves as person identification data of the person requesting a public key certificate, executes a person authentication by

comparing the sampling information against a template obtained from the person identification certificate, and notifies said certificate authority of a success of the person authentication, said certificate authority issuing a public key certificate for the requesting person in response thereto.

3. A public key certificate using system according to Claim 1, wherein said person identification certificate authority executes a mutual authentication with said certificate authority on condition that the person authentication is established on the basis of the person identification certificate of the person requesting a public key certificate, and transmits a public key of the person requesting a public key certificate to said certificate authority on condition that the mutual authentication is established, said certificate authority issuing a public key certificate associated with the public key received.

4. A public key certificate using system according to Claim 1, wherein the public key certificate issued by said certificate authority is a one-time public key certificate which is effective only for a single processing session involving use of an associated public key, based on the person authentication on the basis of the person

identification certificate.

5. A public key certificate using system according to Claim 1, wherein each of said person identification certificate authority and said certificate authority is implemented by a third party which is not in association with a user of the public key certificate and the person identification certificate.

6. A public key certificate using system according to Claim 1, further comprising an authentication requesting device for requesting the person authentication,

wherein the person authentication is executed on the basis of user-entered sampling information transmitted from said authentication requesting device to said person identification certificate authority, the transmission of the user-entered sampling information being executed on condition that a mutual authentication is established between said authentication requesting device and said person identification certificate authority.

7. A public key certificate using system according to Claim 1, further comprising a user device for issuing a service request to a service provider,

wherein said user device transmits user-entered

sampling information to said person identification certificate authority, said person identification certificate authority executes the person authentication by comparing the sampling information against the template obtained from the person identification certificate, said certificate authority issues a public key certificate for the user to said user device on condition that the person authentication is established, and said user device, upon receiving the public key certificate, issues a service request including the public key certificate and transmits the service request to said service provider.

8. A public key certificate using system according to Claim 1, further comprising a user device comprising storage means, used by the person requesting a public key certificate,

wherein said certificate authority issues the public key certificate to said user device, the public key certificate being stored in said storage means, and said user device deletes the public key certificate upon completion of a processing session involving use of the public key certificate stored in said storage means.

9. A public key certificate using system according to Claim 1, further comprising a user device comprising storage

means, used by the person requesting a public key certificate,

wherein said certificate authority issues the public key certificate to said user device, the public key certificate being stored in said storage means, and said user device deletes the public key certificate, and a public key and a private key associated with the public key certificate, upon completion of a processing session involving use of the public key certificate stored in said storage means.

10. A public key certificate using system according to Claim 1, wherein the template comprises personal biometric information such as fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information, non-biometric information such as a seal, a passport, a driver's license, and a card, any combination of two or more biometric or non-biometric information items, or any combination of one or more biometric or non-biometric information items with a password.

11. A public-key certificate using method for using a public key certificate which functions, in association with digital signature data of a certificate authority added

thereto, as a certificate of a public key for encryption processing, said method comprising the steps of:

executing, at a person identification certificate authority, a person authentication by comparing sampling information which serves as person identification data of a person requesting a public key certificate against a template which serves as person identification data of the person requesting a public key certificate, the template being obtained from a person identification certificate possessed by said person identification certificate authority; and

issuing, at a certificate authority, a public key certificate for the requesting person on condition that the person authentication is established.

12. A public key certificate using method according to Claim 11, wherein said person identification certificate authority obtains sampling information which serves as person identification data of the person requesting a public key certificate, executes a person authentication by comparing the sampling information against a template obtained from the person identification certificate, and notifies said certificate authority of a success of the person authentication, said certificate authority issuing a public key certificate for the requesting person in response

thereto.

13. A public key certificate using method according to Claim 11, wherein said person identification certificate authority executes a mutual authentication with said certificate authority on condition that the person authentication is established on the basis of the person identification certificate of the person requesting a public key certificate, and transmits a public key of the person requesting a public key certificate to said certificate authority on condition that the mutual authentication is established, said certificate authority issuing a public key certificate associated with the public key received.

14. A public key certificate using method according to Claim 11, wherein the public key certificate issued by said certificate authority is a one-time public key certificate which is effective only for a single processing session involving use of an associated public key, based on the person authentication on the basis of the person identification certificate.

15. A public key certificate using method according to Claim 11, wherein each of said person identification certificate authority and said certificate authority is

implemented by a third party which is not in association with a user of the public key certificate and the person identification certificate.

16. A public key certificate using method according to Claim 11, further comprising the step of transmitting user-entered sampling information from an authentication requesting device to said person identification certificate authority on condition that a mutual authentication is established between said authentication requesting device and said person identification certificate authority, the person authentication being executed on the basis of the user-entered sampling information.

17. A public key certificate using method according to Claim 11, further comprising the step of transmitting user-entered sampling information from a user device to said person identification certificate authority,

wherein said person identification certificate authority executes the person authentication by comparing the user-entered sampling information against the template obtained from the person identification certificate,

said certificate authority issues a public key certificate for the user to said user device on condition that the person authentication is established; and

said user device, upon receiving the public key certificate, issues a service request including the public key certificate and transmits the service request to a service provider.

18. A public key certificate using method according to Claim 11,

wherein said certificate authority issues the public key certificate to a user device comprising storage means, used by the person requesting a public key certificate, the public key certificate being stored in said storage means, and said user device deletes the public key certificate upon completion of a processing session involving use of the public key certificate stored in said storage means.

19. A public key certificate using method according to Claim 11,

wherein said certificate authority issues the public key certificate to a user device comprising storage means, used by the person requesting a public key certificate, the public key certificate being stored in said storage means, and said user device deletes the public key certificate, and a public key and a private key associated with the public key certificate, upon completion of a processing session involving use of the public key certificate stored in said

storage means.

20. An information processing apparatus comprising:

means for receiving a public key certificate which is issued to a user on condition that a person authentication is established by a person identification certificate authority by comparing sampling information of a user against a template obtained from a person identification certificate;

means for storing the public key certificate; and

means for deleting the public key certificate upon completion of a processing session involving use of the public key certificate stored in said storage means.

21. An information processing apparatus according to Claim 20, wherein said deleting means deletes the public key certificate, and a public key and a private key associated with the public key certificate, upon completion of a processing session involving use of the public key certificate stored in said storage means.

22. A program providing medium which provides a computer program for executing on a computer system a data processing for using a public key certificate which functions, in association with digital signature data of a

certificate authority added thereto, as a certificate of a public key for encryption processing, said computer program comprising the steps of:

executing a person authentication by comparing sampling information which serves as person identification data of a person requesting a public key certificate against a template which serves as person identification data of the person requesting a public key certificate, the template being obtained from a person identification certificate; and

issuing a public key certificate for the requesting person on condition that the person authentication is established.